TWO QUESTIONS ON POLYNOMIAL DECOMPOSITION

BRIAN K. WYMAN AND MICHAEL E. ZIEVE

Abstract. Given a univariate polynomial $f(x)$ over a ring R, we examine when we can write $f(x)$ as $g(h(x))$ where g and h are polynomials of degree at least 2. We answer two questions of Gusić regarding when the existence of such g and h over an extension of R implies the existence of such g and h over R.

1. Introduction

Let R be a ring. If $f(x) \in R[x]$ has degree at least 2, we say that f is *decomposable* (over R) if we can write $f(x) = g(h(x))$ for some nonlinear $g, h \in R[x]$; otherwise we say f is indecomposable. Many authors have studied decomposability of polynomials in case R is a field (see, for instance, [1, 2, 4, 5, 8, 9, 10, 13, 14, 15, 16, 17, 21, 22]). The papers [6, 7, 12] examine decomposability over more general rings, in the wake of the following result of Bilu and Tichy [3]: for $f, g \in R[x]$, where R is the ring of S-integers of a number field, if the equation $f(u) = g(v)$ has infinitely many solutions $u, v \in R$ then f and g have decompositions of certain types. In the present note we answer two questions on this topic posed recently by Gusić [12]:

Question 1.1. *Prove or disprove. Let R be an integral domain of zero characteristic. Let S denote the integral closure of R in the field of fractions of R. Assume that $S \neq R$. Then there exists a monic polynomial f over R that is decomposable over S but not over R.*

Question 1.2. *Prove or disprove. Let R be the ring of integers of a number field K. Assume that R is not a unique factorization domain. Then there exists a polynomial f over R that is decomposable over K but not over R.*

The most significant difference between these questions is that the first question addresses monic polynomials, while the second addresses arbitrary polynomials.

The authors thank Mel Hochster and Alex Mueller for valuable discussions. The authors were partially supported by the NSF under grants DMS-0502170 and DMS-0903420, respectively.

We will show that the first question has a negative answer, and the second has a positive answer. We also pose two new questions along similar lines.

These questions were motivated by two results due to Turnwald [18, Prop. 2.2 and 2.4], which assert that if R is an integral domain of characteristic zero, and K is a field containing R, then:

(1) If R is integrally closed in its field of fractions, then every indecomposable monic polynomial over R is indecomposable over K.
(2) If R is a unique factorization domain, then every indecomposable polynomial over R is indecomposable over K.

The special case $R = \mathbb{Z}$ of Turnwald's first result was first proved by Wegner [19, p. 9], and was later rediscovered in [6, Thm. 2]. Both of Turnwald's results were rediscovered in [12, Thm. 2.1 and 2.5].

Further results about polynomial decomposition over rings appear in the first author's thesis [20] and in forthcoming joint papers by the authors.

2. Monic polynomials

In this section we show that Question 1.1 has a negative answer. We prove this by means of the following result.

Proposition 2.1. *Let S be an integral domain of characteristic zero, and let R be a subring of S. If monic $g, h \in xS[x]$ satisfy $g(h(x)) \in R[x]$, then $g, h \in (\mathbb{Q}.R)[x]$.*

Proof. Write $g = \sum_{i=1}^{n} g_i x^i$ and $h = \sum_{i=1}^{m} h_j x^j$, with $g_n = h_m = 1$. Then, for $1 \le k < m$, the coefficient of x^{nm-k} in $g(h(x))$ is nh_{m-k} plus a polynomial (with integer coefficients) in $h_{m-k-1}, h_{m-k-2}, \ldots, h_{m-1}$. Since this coefficient lies in R, it follows by induction on k that each h_{m-k} lies in $\mathbb{Q}.R$. Likewise, for $1 \le k < n$, the coefficient of x^{nm-km} in $g(h(x))$ equals the sum of g_{n-k} and a polynomial (with integer coefficients) in $g_{n-k+1}, g_{n-k+2}, \ldots, g_{n-1}, h_1, h_2, \ldots, h_{m-1}$. Since this coefficient lies in R, induction on k implies that g_{n-k} lies in $\mathbb{Q}.R$, as desired. □

Corollary 2.2. *Let S be an integral domain of characteristic zero, and let R be a subring of S such that $(\mathbb{Q}.R) \cap S = R$. Then every indecomposable monic polynomial over R is indecomposable over S.*

Proof. Let $f \in R[x]$ be a monic polynomial which is decomposable over S. Say $f = G(H(x))$ where $G, H \in S[x]$ are nonlinear. Denoting the leading coefficients of G and H by u and v, we compute the leading coefficient of f as $1 = uv^{\deg(G)}$. Now let $g = G(vx + H(0)) - f(0)$

and $h = uv^{\deg(G)-1}(H(x) - H(0))$, so g and h are nonlinear monic polynomials in $xS[x]$ such that $g(h(x)) = f(x) - f(0)$ lies in $R[x]$. By the previous result, g and h have coefficients in $\mathbb{Q}.R$; since they also have coefficients in S, in fact their coefficients lie in $(\mathbb{Q}.R) \cap S = R$, so f is decomposable over R. $\square$

We now exhibit an explicit example showing that Question 1.1 has a negative answer. In light of the above corollary, it suffices to exhibit an integral domain R of characteristic zero whose integral closure S satisfies $S \neq R$ and $(\mathbb{Q}.R) \cap S = R$. One example is $R = \mathbb{Z}[t^2, t^3]$, where t is transcendental over $\mathbb{Q}$. The field of fractions of R is $\mathbb{Q}(t)$, and the integral closure of R in $\mathbb{Q}(t)$ is $S := \mathbb{Z}[t]$, so indeed $S \neq R$ and $(\mathbb{Q}.R) \cap S = R$. $\square$

In view of Corollary 2.2 (and Turnwald's result), we pose the following modified version of Question 1.1:

Question 2.3. *Let R be an integral domain of characteristic zero, and let S be the integral closure of R in its field of fractions. If $(\mathbb{Q}.R) \cap S \neq R$, then does there exist an indecomposable monic polynomial over R which decomposes over S?*

Remark 2.4. If R is a subring of a number field K, then $\mathbb{Q}.R = K$; hence, for such rings, Question 2.3 reduces to Question 1.1. It would be interesting to know whether these questions have an affirmative answer in this case.

3. Non-monic polynomials

In this section we show that Question 1.2 has a positive answer.

Theorem 3.1. *If R is the ring of integers of a number field K, and R is not a unique factorization domain, then there exists an indecomposable polynomial over R which decomposes over K.*

In fact we prove the following more general result.

Theorem 3.2. *Let R be an integral domain which contains an element having two inequivalent factorizations into irreducibles, and suppose that every nonsquare in R remains a nonsquare in the fraction field K of R. Then there is an indecomposable degree-4 polynomial over R which decomposes over K.*

Recall that two factorizations into irreducibles are *inequivalent* if there is no bijective correspondence between the irreducibles in the first and the irreducibles in the second such that corresponding irreducibles are unit multiples of one another.

Proof that Theorem 3.2 implies Theorem 3.1. Let R be the ring of integers of a number field K, and suppose that R is not a unique factorization domain. By induction on the norm, every element of R which is neither zero nor a unit can be written as the product of irreducible elements. Thus, since R is not a unique factorization domain, R must contain an element which has two inequivalent factorizations into irreducibles.

Let u be an element of R which is a square in K. Then the polynomial $x^2 - u$ has a root in K, but this is a monic polynomial over R so its roots are integral over R; hence these roots lie in R since R is integrally closed in K. □

Proof of Theorem 3.2. Pick an element of R having two inequivalent factorizations into irreducibles. By repeatedly removing irreducibles from the first factorization which have a unit multiple in the second factorization, we obtain an element $\alpha \in R \setminus (\{0\} \cup R^*)$ having two factorizations into irreducibles such that no irreducible in the first factorization has a unit multiple in the second factorization. Let ℓ be an irreducible in the first factorization, and write the second factorization as $p_1 \dots p_r$ where no p_i is a unit multiple of ℓ. Letting s be the least positive integer for which $\ell \mid p_1 \dots p_s$, it follows that $a := p_1 \dots p_{s-1}$ is an element of R such that $\ell \mid ap_s$ but ℓ does not divide either a or p_s.

Let $c = a/\ell$ and $d = p_s^2$, and put

$$f(x) := (dx^2 + \ell x) \circ (x^2 + cx) = dx^4 + 2dcx^3 + (dc^2 + \ell)x^2 + \ell cx, \tag{3.3}$$

so f is decomposable over K. Note that f has coefficients in R, since ap_s/ℓ lies in R.

Pick nonlinear $g, h \in K[x]$ such that $g \circ h = f$. Let $\mu \in K[x]$ be a linear polynomial such that $\mu \circ h$ is monic and has no constant term. Then $f(x) = (g \circ \mu^{-1}) \circ (\mu \circ h)$, and since $f(0) = 0$ it follows that $g \circ \mu^{-1}$ has no constant term. By inspecting (3.3), we see that the coefficients of f uniquely determine the coefficients of $g \circ \mu^{-1}$ and $\mu \circ h$, so $g \circ \mu^{-1} = dx^2 + \ell x$ and $\mu \circ h = x^2 + cx$. Writing $\mu = u^{-1}x + v$, it follows that there exist $u \in K^*$ and $v \in K$ such that

$$g = \frac{d}{u^2}x^2 + \frac{2dv + \ell}{u}x + (dv^2 + \ell v) \qquad \text{and} \qquad h = ux^2 + ucx - uv.$$

If we can choose such g and h with coefficients in R, then R contains $\{u, uc, uv, d/u^2, (2dv + \ell)/u\}$, so R contains $\ell/u = (2dv + \ell)/u - 2(uv)(d/u^2)$. But R contains $d/u^2 = (p_s/u)^2$, so our hypothesis implies that R contains p_s/u. Thus u divides both ℓ and p_s (in R); since ℓ and p_s are non-associate irreducibles, we must have $u \in R^*$. Finally, since

$uc \in R$, it follows that R contains $c = a/\ell$, contradicting the fact that $\ell \nmid a$. Therefore $f \in R[x]$ is decomposable over K but not over R. $\square$

Remark 3.4. A positive answer to Question 1.2 is provided via a different argument in [18, Prop. 2.6].

We do not know how far Theorem 3.2 can be generalized. We pose the following modification of Question 1.2:

Question 3.5. *Let R be an integral domain of characteristic zero which is not a unique factorization domain, and let K be a field containing R. Does there exist an indecomposable polynomial over R which decomposes over K?*

4. Final note

There is a mistake in [12, Remark 1.2], which attempts to show that if K is a field of characteristic zero, and nonconstant $g, h, G, H \in K[x]$ satisfy $g \circ h = G \circ H$ and $\deg h = \deg H$, then there exist $a, b \in K$ such that $H = ah + b$. The argument in [12] relies on an incorrect assertion, of which a special case says that the sum of a quadratic and cubic polynomial over K cannot equal the sum of a linear and cubic polynomial over K. Since the strategy of the argument is novel, we give here a corrected version of the proof (and we thank I. Gusić for clarifying what was being attempted in [12]).

Write $H = ah + h_0$ with $a \in K$ and $\deg(h_0) < \deg(H)$. We will show that h_0 is a constant polynomial. For, if $h_0 \neq 0$ then Taylor expansion yields

$$g \circ h = G \circ (ah + h_0) = \sum_{i=0}^{m} (G^{(i)} \circ h_0) \frac{(ah)^i}{i!},$$

where $m := \deg(G)$. The left side is a K-linear combination of powers of h, and the right side is the sum of polynomials of degrees $(m - i)\deg(h_0) + i\deg(h)$ for $0 \leq i \leq m$. Moreover, the polynomial of degree $m\deg(h)$ in the latter sum is ch^m for some $c \in K^*$. After subtracting ch^m from both sides, the right side has degree $\deg(h_0) + (m-1)\deg(h)$, while the left side has degree divisible by $\deg(h)$. Thus $\deg(h)$ divides $\deg(h_0)$, and since $0 \leq \deg(h_0) < \deg(H) = \deg(h)$ we conclude that $\deg(h_0) = 0$.

We close by remarking that this result was first proved by Ritt [15] in case $K = \mathbb{C}$, via Riemann surface techniques, and was later proved by Levi [13] by explicitly computing the coefficients of $g \circ h$ (see also [11, Lemma 2.3]). The result can also be proved by means of formal Laurent series [14] or inertia groups [22, Cor. 2.9].

References

[1] R. M. Beals, J. L. Wetherell and M. E. Zieve, *Polynomials with a common composite*, Israel J. Math. **174** (2009), 93–117, arXiv:0707.1552.
[2] A. F. Beardon and T. W. Ng, *On Ritt's factorization of polynomials*, J. London Math. Soc. **62** (2000), 127–138.
[3] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.
[4] A. Bremner and P. Morton, *Polynomial relations in characteristic p*, Quart. J. Math. Oxford Ser. 2 **29** (1978), 335–347.
[5] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.
[6] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–2001.
[7] A. Dujella and R. F. Tichy, *Diophantine equations for second-order recursive sequences of polynomials*, Q. J. Math. **52** (2001), 161–169.
[8] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.
[9] M. D. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. **264** (1973), 40–55.
[10] M. D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.
[11] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math. **171** (2008), 463–483, arXiv:0705.1954v2.
[12] I. Gusić, *On decomposition of polynomials over rings*, Glas. Mat. Ser. III **43** (63) (2008), 7–12.
[13] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.
[14] A. McConnell, *Polynomial subfields of $k(x)$*, J. Reine Angew. Math. **266** (1974), 136–139.
[15] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.
[16] A. Schinzel, Polynomials with Special Regard to Reducibility, Cambridge University Press, 2000.
[17] P. Tortrat, *Sur la composition des polynômes*, Colloq. Math. **55** (1988), 329–353.
[18] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A **58** (1995), 312–357.
[19] U. Wegner, *Über die ganzzahligen Polynome, die für unendlich viele Primzahlmoduln Permutationen liefern*, dissertation, Berlin, 1928.
[20] B. K. Wyman, *Polynomial decomposition over rings*, dissertation, Michigan, 2010.
[21] U. Zannier, *Ritt's second theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), 175–203.
[22] M. E. Zieve and P. Mueller, *On Ritt's polynomial decomposition theorems*, submitted for publication, arXiv:0807.3578v1.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA
Current address: PNYLAB, LLC, 902 Carnegie Center, Suite 200, Princeton, NJ 08540–6530, USA
E-mail address: brian@pnylab.com

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA
E-mail address: zieve@umich.edu
URL: www.math.lsa.umich.edu/∼zieve/